一种基于复合混沌序列的图像加密方法 *

张晓博 [1,2]，彭进业 [1]，习 敏 [3]

(1. 西北工业大学 电子信息学院，西安 710072; 2. 长安大学 信息工程学院，西安 710064; 3. 西安交通大学 电子与信息工程学院，西安 710049)

摘 要：针对低维度混沌系统的密钥空间小，加密系统安全性较低的不足。提出一种由 Sine 混沌改变均匀分布 Logistic 混沌排列次序形成复合混沌序列的图像加密方法。首先，产生服从均匀分布的 Logistic 混沌序列，用 Sine 混沌序列重排该序列整数化后的重复部分，以此无重复数值的复合混沌序列进行像素位置置乱；之后，由于仅进行位置置乱不能改变图像的灰度统计直方图特征，用 Sine 混沌重排整个 Logistic 混沌序列形成复合混沌序列，以此进行像素扩散完成图像加密。对方法安全性从密钥空间、密钥敏感性、差分分析、统计直方图、相邻像素相关性、信息熵方面进行了测量。实验结果表明该方法密钥空间大、敏感性高，能有效地抵抗穷举分析、差分分析和统计分析。

关键词：图像加密；均匀分布；Logistic 混沌；Sine 混沌

中图分类号：TP309.7 doi: 10.3969/j.issn.1001-3695.2018.05.0393

Image encryption algorithm based on complex chaotic sequences

Zhang Xiaobo[1, 2], Peng Jinye[2], Xi Min[3]

(1. *School of Electronic Information*, *Northwestern Polytechnical University*, *Xi'an* 710072, *China*; 2. *School of Information Engineering*, *Chang'an University*, *Xi'an* 710064, *China*; 3. *School of Electronics & Information Engineering*, *Xi'an Jiaotong University*, *Xi'an* 710049, *China*)

Abstract: For the low dimensional chaotic system, the key space is small and the security of the encryption system is low. This paper presents an image encryption method for complex chaotic sequences formed by Sine chaos changing uniformly distributed Logistic chaos order. First, a Logistic chaotic sequence obeying uniform distribution is generated. Sine chaotic sequence is used to rearrange the repeated part after the integer of the sequence, so that the compound chaotic sequence without repeating value is used for pixel position disorder. After that, because position scrambling alone cannot change the histogram features of gray statistics of the image, Sine chaos was used to rearrange the entire Logistic chaos sequence to form compound chaotic sequence, so as to complete image encryption by pixel diffusion. The method security was measured from key space, key sensitivity, differential analysis, statistical histogram, adjacent pixel correlation and information entropy. The experimental results show that this method has a large key space and high sensitivity, and can effectively resist exhaustive analysis, differential analysis and statistical analysis.

Key words: Image encryption; uniform distribution; Logistic chaos; sine chaos

0 引言

随着互联网技术的日趋成熟与信息技术的发展，越来越多的信息被数字化通过网络传播，这些信息的形式有文字、图像、视频等。图像由于直观、生动的特点被广泛用于信息传播和交换。在日趋复杂的网络环境中保证传输图像的安全性和保密性具有重要意义。对具有数据量大、像素间存在相关性等特点的图像数据，IDEA、AES 和 DES 等主要面向文本加密的方法不具优势[1,2]。

混沌系统产生的连续信号经离散化后形成混沌序列，具有不可预测性、非周期性等特点，在图像加密领域具有突出优势，基于混沌系统的图像加密成为研究热点[3]。文献[4]提出使用 Logistic 映射和二维 Henon 映射，通过图像位置置乱和像素灰度值加密两个步骤完成加密。文献[5]使用 Logistic 映射分别进行位置置乱和灰度值扩散。文献[6]对每个像素点进行一次位置置乱后紧接着进行一次扩散。这些方法相较于单一的位置置乱，

收稿日期：2018-05-29；**修回日期：**2018-08-02 **基金项目：**中央高校基本科研业务费专项资金资助项目（CHD2011JC101））；国家自然科学基金青年项目（61101215/F010401）

作者简介：张晓博（1975-），男，陕西西安人，讲师，博士研究生，主要研究方向为模式识别与图像处理（xbzhang@chd.edu.cn）；彭进业（1964-），男，湖南涟源人，教授，博士，主要研究方向为模式识别、信号与信息处理；习敏（1994-），女，陕西渭南人，硕士研究生，主要研究方向为模式识别.

不但改变了像素位置而且改变了像素灰度值分布，增大了破译难度。但上述方法使用的 Logistic 混沌的统计特性不服从均匀分布，密文的隐藏性有一定不足。

混沌加密的安全性很大程度上依赖于混沌序列的分布性、随机性和复杂性[7]，对基本混沌序列进行改造是有益的。文献[8]针对 1 维 Logistic 映射只有两个可变参数的不足，提出了一种基于 3 维交织编码 Logistic 映射产生混沌序列的方法。文献[9]提出了一种 Logistic 映射和双随机相位编码结合的彩色图像加密方法。文献[10]提出由 Logistic 映射和蔡氏电路（Chua's circuit）组成 Logistic-Chua 复合混沌映射产生混沌序列的方法。文献[11]使用 Logistic、Ten 和 Sine 等混沌映射两两之间进行异或、取模和反馈操作形成新的复合混沌。文献[12]对 Logistic 混沌序列进行均匀化，并在此基础上通过序列元素的位置交换实现一种 Logistic 随机排列的生成方法（Logistic random permutation based on position interchange, LRPRI），该方法对均匀分布的 Logistic 序列，首先从以 1,2，…，n 排列的序列中任选一个位置的数与最后位置 n 上的数进行位置互换；之后从余下的 1,2，…，n-1 序列中再随机选择一个数与 n-1 位置上的数互换，直到结束。该方法通过对均匀分布 Logistic 序列进行位置交换，进一步增加了 Logistic 的无序性，但使用单一混沌序列作为密钥序列的安全性有待提高。

在文献[11,12]的基础上，本文提出了一种复合混沌序列生成方法。首先产生一个服从均匀分布的 Logistic 混沌序列，再依据 Sine 混沌序列的数值大小次序来重新排列 Logistic 序列中元素的排列位置，以形成复合混沌序列。方法通过不同类型的混沌序列来改变混沌序列的排列次序，既保持原有混沌序列的均匀分布特性，又通过重新排序 Logistic 序列形成复合混沌，增强了密钥序列的无序程度。

本文的加密过程包括位置置乱和像素扩散两步。在位置置乱中，为了避免在将混沌序列值转换为整数时，由于取整的舍入误差引起的重复数值。提出用 Sine 序列重排部分 Logistic 序列次序的无重复数值的复合混沌序列生成方法。在像素扩散中，为了进一步增大 Logistic 序列的无序性，依据 Sine 序列值大小的排序重排全部 Logistic 序列的排列次序，生成像素扩散用复合混沌序列。经实验，本文方法能有效地抵抗穷举分析、统计分析和差分分析等攻击类型。

1　混沌序列

基于混沌序列的图像加密通常是将混沌序列与原图像信息进行异或、循环移位等运算，使原图像信息变为具有类似随机噪声的性态，达到加密目的。以下是本文用到的混沌序列。

1.1　基本 Logistic 混沌序列

混沌在动力学系统中指确定性动力学系统因对初值敏感而表现出的不可预测、类似随机性的运动。在图像处理领域常使用 Logistic 混沌映射进行图像加密。Logistic 混沌映射是一种动力系统，系统方程为

$$x_{i+1} = \mu x_i (1 - x_i) \tag{1}$$

其中：$x_i \in V, i = 0,1,2,\dots$，称为状态，$x_0$ 是初值，μ 为混沌系统的李雅普诺夫(Lyapunov)指数，取值区间为 $(0,4]$。当 Lyapunov 指数 μ 在区间（3.5699456,4.0]时，Logistic 映射呈混沌状态，其迭代生成的序列值处于一种随机分布的状态，系统状态的值域 $x_i \in (0,1)$。

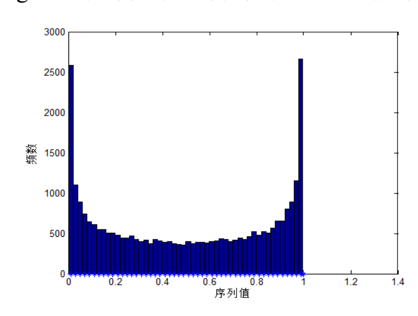
基本的 Logistic 映射所产生的序列是非均匀分布的，直接用于图像加密存在一定安全隐患。

1.2　服从均匀分布的混沌序列

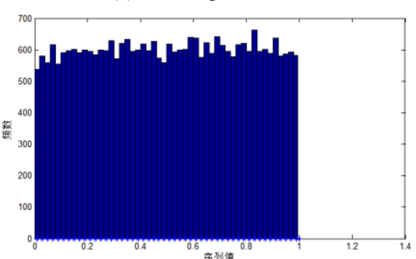
目前已有一些将混沌序列转换为具有均匀分布统计特性序列的研究[12~14]，本文采用序列映射的方法进行转换[12]。对于基本 Logistic 混沌序列 x_1 按式（2）映射转换为服从均匀分布的混沌序列序列 x_2，算式如下：

$$x_2 = \frac{2}{\pi} \arcsin \sqrt{x_1} \tag{2}$$

转换后，序列 x_2 为区间 (0,1) 上服从均匀分布的随机变量。由 μ 为 3.997，x_0 为 0.512，迭代 30000 次产生 Logistic 序列的序列值分布直方图如图 1（a）所示，根据式（2）转换后服从均匀分布的 Logistic 序列统计直方图如图 1（b）所示。



(a)基本 Logistic 序列



(b)均匀化后 Logistic 序列

图 1　Logistic 序列统计直方图

从图 1 (b)序列值出现频数的统计直方图可以看出，经过映射转换后的 Logistic 序列在（0,1）区间序列值的出现机率是均等的。

1.3　Sine 混沌序列

用于构造复合混沌序列的 Sine 映射的表达式为

$$x_{n+1} = \frac{a}{4} \sin(\pi x_n) \qquad 0 < a \le 4 \tag{3}$$

其中：系统参数 α 的取值范围∈(0,4]。由于 Sine 函数的值域区间是[-1,1]，在根据其序列值大小进行重排其他序列次序时运算快捷，因此选择由 Sine 混沌来改变 Logistic 混沌序列的排列次序以构成复合混沌序列。

2 图像像素位置置乱

像素位置置乱的目的是从图像空间位置上掩盖明文、密钥和密文之间的关系。方法用无重复数值的复合混沌序列作为置乱密钥序列，改变图像的像素点位置，实现位置置乱。

2.1 无重复数值置乱密钥序列

本文在均匀分布 Logistic 序列的基础上提出一种无重复数值的复合混沌序列实现方法。方法用 Sine 类型的混沌序列改变均匀分布 Logistic 序列的排列，形成新的复合混沌序列。考虑到若直接用此复合混沌序列进行图像位置置乱，需要将取值范围是（0,1）之间浮点数的 Logistic 序列与图像像素坐标对应，通常做法是将序列值乘以图像的大小后再取整数。浮点数取整数是根据四舍五入进行取整，会出现相当数量的相同整数。使用具有相同整数的序列去改变明文图像像素位置时，其所对应像素的位置不会被移动，达不到置乱目的。为解决这个问题，提出无重复数值的置乱密钥序列产生方法，即用 Sine 混沌序列替换整数化后 Logistic 序列中重复数值，生成加密用的复合混沌序列，步骤如下：

a）对大小为 M×N 图像，产生一组长度均为 L 的 Logistic 序列 x_1，用式（2）转换为均匀 Logistic 序列。为保证混沌性，截取从 200 点之后长度为 M×N 的部分，记为序列 m1。

b）由于 m1 取值范围是（0,1）之间的浮点数，为了和被置乱图像的像素位置对应，将 m1 中的每个元素值乘以（M×N-1），再加 1 使序列中每个数值改变为(1,M×N)之间的浮点数，记为序列 m2。

c）用四舍五入的方法将序列 m2 中的数值转换为整数，会在序列中产生相当数量的重复数值。将重复出现的数值只保留第一次出现时对应序列位置上的数值，之后再次出现的序列值被置为 0，并记录重复出现的数值的总数 S，及其在 m2 中的位置；

d）用 Sine 映射产生一组长度为 S 的混沌序列，序列的值为[-1,1]。

e）将 Sine 混沌序列的值按照大小进行升序排列，并用一维数组 R 记录新序列中每个值在原序列中的位置。

f）将 m2 中没有出现在[1,M×N]之间的数值，依照数组 R 的次序插入步骤 3 中被置为 0 的序列位置上。

通过以上步骤得到长度为 M×N，取值范围为[1,M×N]且值为互不相同整数的序列 m3，以 m3 作为位置置乱密钥序列。

以图像大小 M×N 为 256×256 图像的置乱密钥序列生成进行说明。密钥序列的参数为 $[\mu, x_1(0), \alpha, x_2(0)]$，其中 μ 为 Logistic 混沌的 Lyapunov 指数，$x_1(0)$ 为初值；α 为 Sine 函数系数，$x_2(0)$ 为初值，数值取[3.9997, 0.512,4.0,0.88]。首先，产生长度为 65536 的均匀分布 Logistic 序列，每个序列值乘以图像大小 M×N，转换为 32 位无符号整数序列；此时，序列由于取整舍入产生了 24400 个重复的数值；之后，记录这些重复位置上的数值和在 Logistic 序列中的位置；最后，生成长度为 24400 的 Sine 混沌序列，依照 Sine 序列值的升序，将上一步 1~65536 中没有出现的 24400 的数重新填入到这些重复位置中，产生一个和图像大小相等，且数值为 1 至 65536 的无重复数值的整数序列。序列值的排列次序是由 Logistic 和 Sine 混沌序列共同决定，其序列值如图 2 所示。

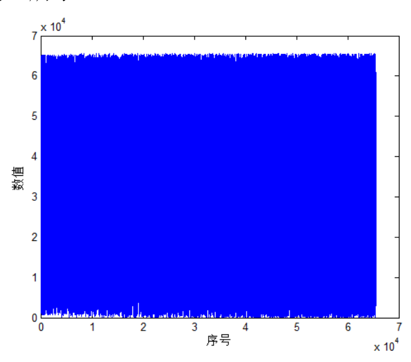


图 2 无重复数值置乱密钥序列

图 2 中，序列长度和图像的大小一致，均为 65536，序列的值为 1-65536，且每个值只出现一次。

2.2 图像像素位置置乱

图像像素位置置乱通过密钥序列打乱原图像的像素位置。本文提出无重复数值的置乱密钥生成后，像素位置置乱的步骤得到简化，只需以下四步：

a) 依照 2.1 节方法用 Logistic 混沌和 Sine 混沌序列产生无重复数值的整数密钥序列。

b）将图像转换为一维序列。

c)将一维序列中每个元素按照生成的整数密钥序列中对应元素内的值作为移动目标位置依次进行移动。

d）转换一维序列为二维，完成图像的像素点位置置乱。

3 图像像素扩散

图像像素点置乱通过移动图像中像素点的位置，从视觉上掩盖原图像内容，但像素点的灰度值没有改变，加密后图像和原图像的灰度统计直方图一致，存在安全隐患。有必要通过像素扩散隐藏图像的统计直方图特性，即在不改变像素点位置的情况下，将任一像素点的信息隐藏在其他的密文像素点中。

3.1 扩散密钥序列生成

扩散密钥序列采用和置乱密钥相似的复合混沌序列产生方法。为了进一步增加密钥序列的无序程度，相对于置乱序列是使用 Sine 序列改变出现重复数值的 Logistic 序列中部分位置的排列次序，扩散序列是使用 Sine 序列改变整个 Logistic 序列的排列次序，步骤如下：

a）产生长度与图像大小 M×N 相同的一维 Logistic 均匀混沌序列。

b）产生长度为 M×N 的 Sine 混沌序列，序列的值为[-1,1]。

c）将 Sine 混沌序列的元素按照升序排列，并用一维数组 A 记录新序列中每个元素在原 Sine 序列中的位置。

d）用 Sine 混沌序列重新排列 Logistic 序列，即将 Logistic 序列按照一维数组 A 的值重新排列，得到像素扩散所用的复合

混沌序列 S。

3.2　基于双向循环异或运算的像素扩散

在扩散密钥序列生成后，用双向循环异或运算进行像素扩散，即对图像每一像素进行正向循环和逆向循环共两次异或运算，将明文图像中某一点像素的信息扩散到整个密文像素中[15]。

像素扩散的过程：先将大小为 M×N 的灰度图像 $I_{M\times N}$，转为成长度为 M×N 的一维向量 P，其值与 3.1 节产生的长度为 M×N 的密钥序列 S 一一对应，再依次进行正向和逆向异或运算两次循环，得到以一维向量表示的密文 C。其中，正向（即 i 从 1 到 MN）循环的异或运算如式（4）所示，对应的解密逆运算如式（5）所示。

$$C_i = C_{i-1} \oplus S_i \oplus P_i \tag{4}$$

$$P_i = C_{i-1} \oplus C_i \oplus S_i \tag{5}$$

如式（4）所示，进行正向循环后，P_1 像素点的信息可以扩散到全部密文像素点的信息中，但 P_2 像素点的信息只能扩散到 $C_2 \sim C_{MN}$，即明文像素点 P_i 的信息只能扩散在 $C_i \sim C_{MN}$ 中，扩散的效果不佳。因此，需要按逆向（即 i 从 MN 到 1）循环一次，即按照式（6）循环。其对应的解密的逆运算如式（7）所示。

$$C_i = C_{i+1} \oplus S_i \oplus P_i \tag{6}$$

$$P_i = C_{i+1} \oplus C_i \oplus S_i \tag{7}$$

4　加密解密过程

当混沌系统由两个以上混沌序列组成时，其非线性行为更加复杂和难以预测[16]。本文的密钥序列由均匀分布 Logistic 混沌和 Sine 混沌组成，密钥序列的生成方法如第 3 节所述，其参数为 $[\mu, x_1(0), \alpha, x_2(0)]$，其中 μ 为 Logistic 混沌 Lyapunov 指数，$x_1(0)$ 为初值；α 为 Sine 函数系数，$x_2(0)$ 为初值，加密与解密过程如下：

4.1　加密过程

加密过程包括像素位置置乱和灰度值扩散两步。首先，产生均匀分布 Logistic 混沌序列并整数化，用 Sine 混沌序列改变其部分序列的排列产生无重复数值的混沌序列，以此序列对图像进行像素点位置置乱。之后，用同样的密钥参数产生均匀分布 Logistic 混沌序列，用 Sine 混沌序列改变整个 Logistic 序列的排列，以此序列和置乱后图像进行正向和逆向扩散运算，完成像素灰度值扩散，实现图像加密。

4.2　解密过程

图像的解密过程是加密的逆过程，解密密钥的参数与加密密钥参数 $[\mu_1, x_1(0), \mu_2, x_2(0)]$ 相同。解密过程是先进行像素灰度值扩散解密，后进行像素点位置置乱解密，完成从密文中恢复图像。

5　实验与结果

选择 Cameraman、Lena、Peppers 灰度图像作为测试图像进行加密和解密实验。实验采用 Logistic 和 Sine 混沌的系统参数和初值 $[\mu_1, x_1(0), \mu_2, x_2(0)]$ 作为密钥，取值为 [3.9997, 0.512,4.0,0.88]。使用计算机为 i5 CPU，软件是 MATLAB2014。实验中，加密过程用时平均为 0.153 s，解密过程用时平均为 0.151 秒，实验的视觉效果如图 3 所示。

图 3 中，（a）列从上到下依次为 Cameraman 明文图像、灰度直方图与幅度谱，Lena 明文图像、灰度直方图与幅度谱，Peppers 明文图像、灰度直方图与幅度谱；（b）列从上到下依次为 Cameraman 密文图像、灰度直方图与幅度谱，Lena 密文图像、灰度直方图与幅度谱，Peppers 密文图像、灰度直方图与幅度谱；（c）列从上到下依次为解密 Cameraman 图像、灰度直方图与幅度谱，解密 Lena 图像、灰度直方图与幅度谱，解密 Peppers 图像、灰度直方图与幅度谱。

从图 3 的明文、密文和解密后图像可以看出，密文图像的灰度统计直方图基本呈均匀分布，且密文图像灰度值的幅度谱也很平坦，即密文图像的像素值在[0,255]的灰度取值范围内出现的概率几乎均等。

6　算法安全性分析

6.1　密钥空间分析

密钥空间是衡量密码系统安全性的一个重要指标。密钥空间越大，抵御穷举攻击的能力越强。本文以 Logistic 系统参数 μ，初值 α 和 Sine 混沌映射参数 $[\mu, x_1(0), \alpha, x_2(0)]$ 作为密钥。在 32bit 计算机中，依 IEEE 754 标准规定表示双精度浮点数的长度是 64bit，则密钥空间为 $2^{64} \times 2^{64} \times 2^{64} \times 2^{64} = 2^{256}$。从安全的角度，密钥空间≥$2^{100}$≈$10^{30}$ 就能满足较高的安全级别，所以本算法的密钥空间对穷举攻击是安全的。

6.2　密钥敏感性分析

密钥敏感性是指在加密过程中对密钥进行微小变化（如 $\pm 10^{-10}$），能产生与原始密文完全不同的加密密文；同理，在解密过程中，对原始解密密钥进行微小变化（如 $\pm 10^{-10}$），对同一密文能产生完全不同的解密结果[17][18]。

为了评估分析密钥敏感性，对某个密钥作微小的改变，计算通过加密算法得到的对应密文图像的变化率。常用像素数目变化率 NPCR（Number of Pixels Change Rate）与像素强度变化强度 UACI（Unified Average Changing Intensity）测量，其定义分别为

$$NPCR = \frac{\sum_{i,j} Dif(I_1, I_2)}{M \times N} \times 100\% \tag{8}$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|I_1(i,j) - I_2(i,j)|}{255}\right] \times 100\% \tag{9}$$

其中：I_1 是原始密钥加密后的图像，I_2 是密钥有微小改变后的加密图像；$Dif(I_1, I_2)$ 表示图像 I_1 和 I_2 不同像素的个数，其取值是：若 $I_1(i,j) \neq I_2(i,j)$，则 $Dif(I_1, I_2) = 1$，若 $I_1(i,j) \neq I_2(i,j)$，则 $Dif(I_1, I_2) = 0$；M、N 分别为图像 I_1 和 I_2 的长、宽。测试图像 Cameraman 为 8 位灰度图像，其理论值为：NPCR =99.6094%，UACI=33.4635%。

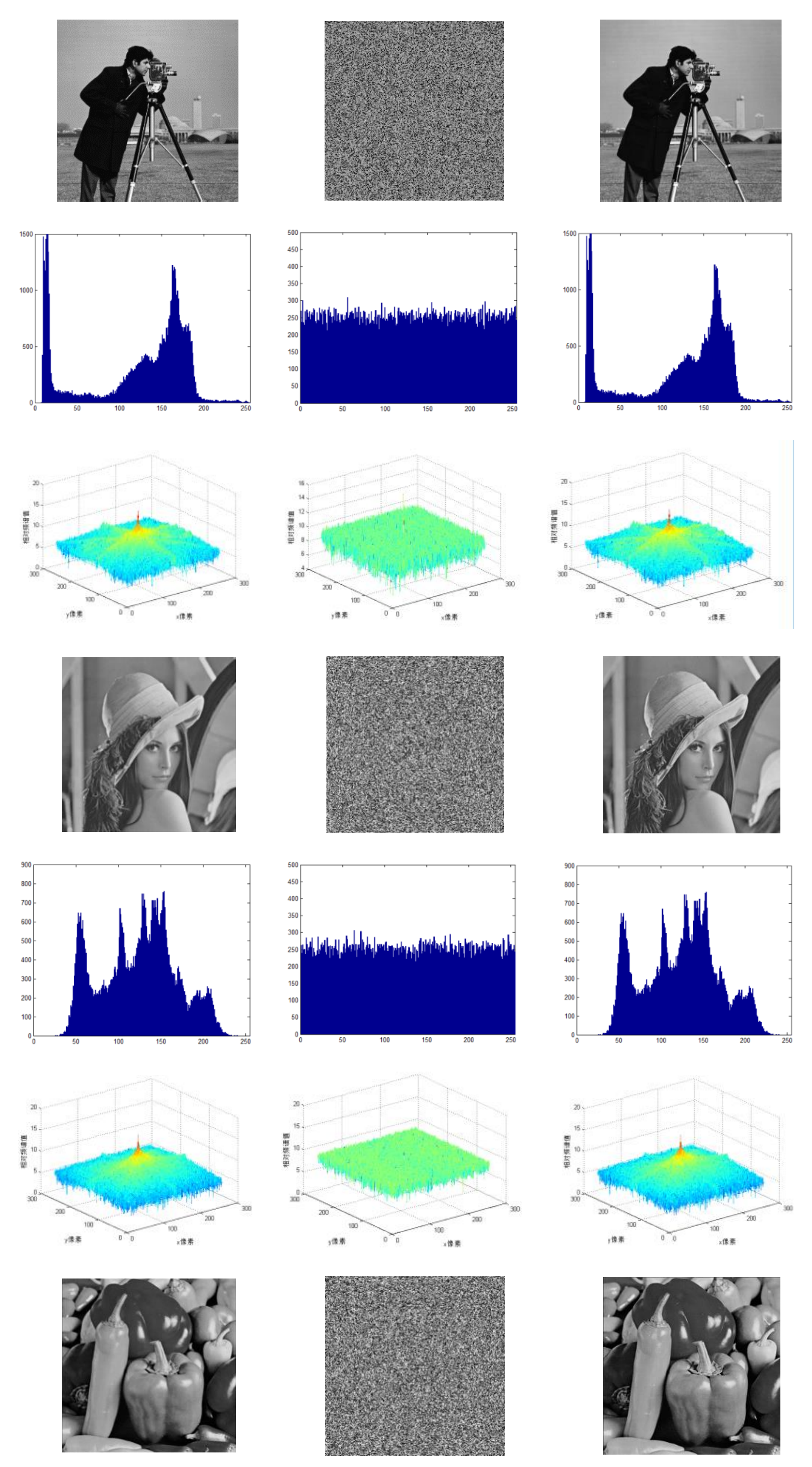


图 3　加密与解密视觉效果图

实验中，对图像 Cameraman 在加密过程的加密密钥做微小变化，使密钥中的混沌系统初值每次增加10^{-10}（表 1 中用Δ表示），测定利用微小变化后的密钥加密生成的密文与原始密文之间的 NPCR 与 UACI 值，结果如表 1 所示。

表 1 加密密钥敏感性测定表

$\Delta\mu$	$\Delta x_1(0)$	$\Delta\alpha$	$\Delta x_2(0)$	NPCR	UACI
1	-	-	-	99.501%	33.107%
2	-	-	-	99.572%	33.116%
-	1	-	-	99.207%	33.075%
-	2	-	-	99.396%	33.125%
-	-	1	-	99.402%	33.013%
-	-	2	-	99.510%	33.035%
-	-	-	1	99.115%	33.023%
-	-	-	2	99.227%	33.031%

表 1 中，测得的 NPCR 与 UACI 值与理想值很接近，说明当密钥发生微小变化时，密文图像中 99%以上的像素会发生改变，攻击者很难用穷举法进行分析。本文的解密过程与加密密过程是对称的，因此对解密密钥可得出相同的结论，即本文方法的密钥敏感性很强。

6.3 差分攻击分析

差分攻击是一种选择明文攻击，攻击者通过对明文进行微小的改变，分析经过相同加密系统后对应密文之间的差别进行攻击。加密系统抵抗差分攻击的能力可通过 NPCR 和 UACI 两个指标衡量[10,19]。实验采用 Cameraman，Lena 和 Peppers 灰度图像，步骤如下：

a)对于明文图像 I，使用加密系统得到对应的密文图像 E_1。

b)从图像 I 中随机选择一个像素点，改变其灰度值，变化量为 1，用同样的密钥和加密系统得到的密文图像记为 E_2。

c)对密文 E_1 和 E_2，计算 NPCR 和 UACI。

d)重复步骤 b）c)共 100 次，得到 NPCR 和 UACI 的平均值。

表 2 是实验得到的 NPCR 和 UACI 平均值，数值接近理论值，加密算法具有较好的抵抗差分攻击的能力。

表 2 差分攻击分析的 NPCR 和 UACI 平均值表

指标	Cameraman	Lena	Peppers
NPCR	99.59	99.60	99.59
UACI	33.45	33.44	33.45

6.4 统计分析

对加密算法进行统计分析的目的是测定算法在置乱和扩散性能方面抵御统计攻击的能力，本文通过分析图像的灰度统计直方图、相邻像素相关性和信息熵实现。

6.4.1 灰度统计直方图

图像的灰度统计直方图通过统计图像中每个灰度级出现的像素次数，表征图像像素的分布特性。加密前后明文图像和密文图像的灰度统计直方图如图 3 所示。从图中可以看出，密文图像直方图是均匀分布的，攻击者几乎无法从统计直方图中分析出统计特性。

6.4.2 相邻像素相关性分析

图像由像素组成，相邻的像素之间由于色彩、明暗的过渡存在一定的关联性。灰度图像可以看成由不同像素的灰度值构成的矩阵，由于相邻像素点之间存在关联性，许多相邻像素的灰度值差值较小。为了提高加密图像的保密性，必须降低密文图像相邻像素之间的相关性[20]。相邻像素相关性系数 ρ_{xy} 的定义如下[20]：

$$p_{xy}=\frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{10}$$

其中：x 和 y 表示图像中两个相邻像素的灰度值大小，cov(x,y)为这两个像素灰度值 x 和 y 的协方差，D(x)和 D(y)分别为 x 和 y 的方差，其计算公式如下：

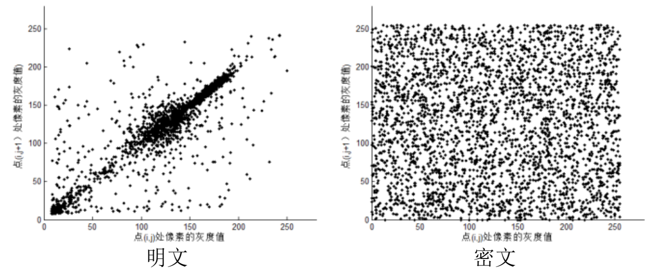
$$E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i \tag{11}$$

$$D(x)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))^2 \tag{12}$$

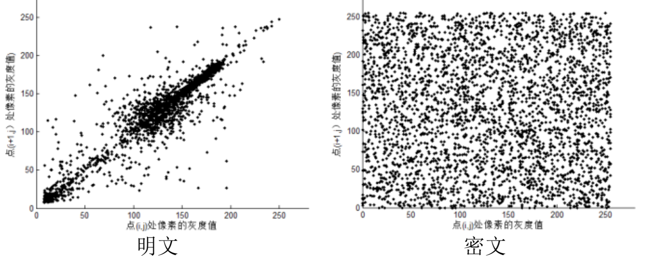
$$\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}(x_i-E(x))(y_i-E(y)) \tag{13}$$

由上述定义式可以看出，相邻像素间的相关性越强，相关性系数 ρ_{xy} 越大。

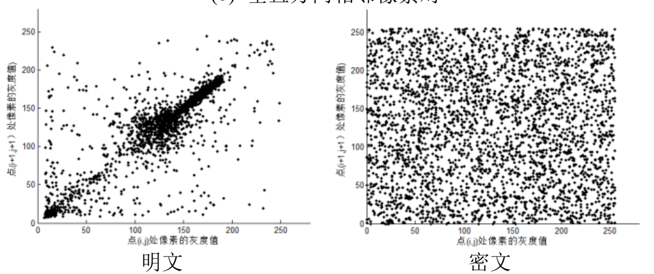
在 Cameraman 明文图像和密文图像中分别随机选取 10%数量的像素点，取其在水平、垂直、对角线方向的相邻像素的灰度分布情况如图 4 所示。



(a) 水平方向相邻像素对



(b) 垂直方向相邻像素对



(c) 对角线方向相邻像素对

图 4 Cameraman 图像明文、密文在不同方向上的相邻像素分布

图 4 中,明文在三个方向上相邻像素的灰度值几乎集中分布在一条直线上，说明相邻位置上每个像素对的灰度值差别不大，相关性强；密文在上述方向上的相邻像素对的灰度值平均分布在整个灰度值范围，接近不相关。因此本文算法能破坏图像相邻像素间的相关性，使密文像素的灰度值在图像平面的分布接近随机，攻击者很难用统计攻击法破解。

表 3 是本文方法图像相邻像素间的平均相关系数的比较。从表 2 可以看出，密文图像相邻像素的平均相关系数较明文图像前明显减小，接近于 0。

表 3　明文和密文相邻像素间的平均相关系数

	Cameraman		Lena		Peppers	
	明文	密文	明文	密文	明文	密文
水平方向	0.9606	-0.0011	0.9774	0.0012	0.9650	-0.0237
垂直方向	0.9322	-0.0050	0.9543	-0.0017	0.9634	0.0054
对角方向	0.9106	-0.0027	0.9304	-0.0028	0.9276	-0.0046

6.4.3 信息熵

信息熵是度量信息不确定度的物理量，计算式如下:

$$H(X) = -\sum_{i=0}^{2^L-1} P(X_i)\log_2 P(X_i) \tag{14}$$

其中：$P(X_i)$ 是信号 X_i 出现的概率，L 是每个信号的比特数，对于图像则表示灰度图像的灰度等级数。信息的不确定性越大，熵值也越大。

实验对 Cameraman 图像进行，该图像是 L=8 的的灰度图像，有 256 级灰度，信息熵的最大值为 8。计算本文方法加密后的 Cameraman 图像信息熵为 7.9895，接近信息熵的最大值，说明加密后的图像信息不确定度很大，能够抵抗熵分析。

7　结束语

本文提出一种新的复合混沌序列的产生方法，并通过像素位置置乱和灰度值扩散的双重加密步骤，实现图像加密。方法的主要特点有：

a）依据 Sine 混沌序列元素的排列次序改变均匀分布 Logistic 混沌序列的排列次序的方法，运算简洁。

b）在位置置乱过程中，用 Sine 混沌重排匀分布 Logistic 序列中部分重复元素的排列次序，生成无重复数值、且与被置乱图像像素位置一一对应的密钥序列，简化了后续置乱步骤。

c）在像素值扩散中，用 Sine 混沌重排全部均匀分布 Logistic 序列的排列次序，较部分打乱进一步提高了序列的无序程度，并通过正向、逆向循环异或操作完成像素扩散。

本文加密方案的置乱和扩散过程都是在空间域进行，对原图像信息保存完整，经过实验验证，能有效抵抗穷举分析，差分分析和统计分析等类型的攻击。

参考文献：

[1] Pareek N K, Patidar V, Sud K K. Image encryption using chaotic logistic map [J]. Image and Vision Computing, 2006, 24 (9): 926-934.

[2] Li Chengqing, Tao Xie, Qi Liu, Cheng Ge. Cryptanalyzing image encryption using chaotic logistic map [J]. Nonlinear Dynamics, 2014, 78 (2): 1545-1551.

[3] Gao Tiegang, Chen Zengqiang. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A, 2008, 372 (4): 394-400.

[4] 张雪锋，范九伦. 一种改进的基于混沌系统的数字图像加密算法 [J]. 计算机应用研究, 2007, 24 (4): 184-186. (Zhang Xuefeng, Fan Jiulun. Extended image encryption algorithm based on chaos system [J]. Application Research of Computers, 2007, 24 (4): 184-186.)

[5] 胡春强，邓绍江，秦明甫，等. 基于 Logistic 与标准映射的数字图像加密算法 [J]. 计算机科学, 2010, 37 (12): 57-59. (Hu Chunqiang, Deng Shaojiang, Qin Mingfu, el at. Image encryption algorithm based on logistic and standard map [J]. Computer Science, 2010, 37 (12): 57-59.)

[6] 舒永录，张玉书，肖迪，等. 基于置乱扩散同步实现的图像加密算法 [J]. 兰州大学学报：自科版, 2012, 48 (2): 113-116. (Shu Yonglu, Zhang Yushu, Xiao Di, *et al.* Image encryption algorithm based on the synchronization of permutation and diffusion. Journal of Lanzhou University: Natural Sciences, 2012, 48 (2): 113-116.)

[7] 朱从旭，胡玉平，孙克辉. 基于超混沌系统和密文交错扩散的图像加密新算法 [J]. 电子与信息学报, 2012, 34 (7): 1735-1743. (Zhu Congxu, Hu Yuping, Sun Kehui. New image encryption algorithm based on hyperchaotic system and ciphertext diffusion in crisscross pattern [J]. Journal of Electronics & Information Technology, 2012, 34 (7): 1735-1743.)

[8] Ye Guodong, Huang Xiaoling. An efficient symmetric image encryption algorithm based on an intertwining logistic map [J]. Neurocomputing, 2017, 251: 45-53.

[9] Huang Huiqing, Yang Shouzhi, Colour image encryption based on logistic mapping and double random-phase encoding [J]. Iet Image Processing, 2017, 11 (4): 211-216.

[10] Slimane N B, Bouallegue K, Machhout M. Designing a multi-scroll chaotic system by operating Logistic map with fractal process [J]. Nonlinear Dynamics, 2017, 88 (3): 1655-1675.

[11] Zhou Yicong, Bao Long, Chen C. L. Philip. A new 1D chaotic system for image encryption [J]. Signal Processing, 2014, 97: 172-182.

[12] 曹光辉，胡凯，佟维. 基于 Logistic 均匀分布图像置乱方法 [J]. 物理学报, 2011, 60 (11): 133-140. (Cao Guanghui, Hu Kai, Tong Wei. Image scrambling based on Logistic uniform distribution [J]. Acta Physica Sinica, 2011, 60 (11): 133-140.)

[13] 盛利元，肖燕予，盛喆. 将混沌序列变换成均匀伪随机序列的普适算法 [J]. 物理学报, 2008, 57 (7): 4007-4012. (Sheng Liyuan, Xiao Yanyu, Sheng Zhe. A universal algorithm for transforming chaotic sequences into uniform pseudo-random sequences [J]. Acta Physica Sinica, 2008, 57 (7): 4007-4012.)

[14] 李佩玥，石俊霞，郭嘉亮，等. 一种混沌伪随机序列均匀化普适算法的改进 [J]. 电子学报, 2015, 43 (4): 753-759. (Li Peiyue, Shi Junxia, Guo Jialiang, el at. Improvement of a Universal Algorithm for Uniformization of Chaotic Pseudo-Random Sequences [J]. Acta Electronica Sinica, 2015, 43

(4): 753-759.)

[15] 张勇，混沌数字图像加密 [M]. 北京：清华大学出版社，2016: 59-60. (Zhang Yong, Chaotic Digital Image Cryptosystem [M] , Bei Jing: Tsinghua University Press, 2016: 59-60.)

[16] 蒋君莉，张雪锋. 基于多混沌系统的彩色图像加密方法 [J]. 计算机应用研究，2014, 31 (10): 3131-3136. (Jiang Junli, Zhang Xuefeng. Color image encryption method based on chaotic systems [J]. Application Research of Computers, 2014, 31 (10): 3131-3136.)

[17] 罗玉玲，杜明辉. 基于量子 Logistic 映射的小波域图像加密算法 [J]. 华南理工大学学报：自然科学版，2013, 41 (6): 53-62. (Luo Yuling, Du Minghui. Image encryption algorithm based on quantum logistic map in wavelet domain [J]. Journal of South China University of Technology: Natural Science Edition, 2013, 41 (6): 53-62.)

[18] Behnia S, Akhshani A, Ahadpour S, et a1. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps [J]. Physics Letters A, 2007, 366: 391-396.

[19] Xu Lu, Li Zhi, Li Jian, Hua Wei. A novel bit-level image encryption algorithm based on chaotic maps [J]. Optics and Lasers in Engineering, 2016, 78 (21): 17-25.

[20] Mohamad Javad Rostam, Abbas Shahba, Saeid Saryazdi, *et al.* A novel parallel image encryption with chaotic windows based on logistic map [J]. Computers and Electrical Engineering, 2017, 62: 384-400.